
Ciscomania Articles

Port-based Authentication

Port-based Authentication

To pass your CCNA exam and earn this coveted certification, you must understand the details of port-based authentication. This knowledge has a great deal of value in production networks as well, since this authentication scheme is regularly implemented. Let's take a look at this particular CCNA skill.

Consider a situation where you have a server that will be connected to your switch, and you want the port to shut down if a device with a different MAC address than that of the switch attempts to connect to that port. You could also have a situation where you have someone who has a connection to a switch port in his office, and he wants to make sure that only his laptop can use that port.

Both of these examples are real-world situations, and there are two solutions for each. First, we could create a static MAC entry for that particular switch port. I don't recommend this, mainly because both you and I have better things to do than manage static MAC entries. The better solution is to configure port-based authentication on the switch.

The Cisco switch uses MAC addresses to enforce port security. With port security, only devices with certain MAC addresses can connect to the port successfully. This is another reason source MACs are looked at before the destination MAC is examined. If the source MAC is non-secure and port-based authentication is in effect, the destination does not matter, as the frame will not be forwarded. In essence, the source MAC address serves as the password.

MAC addresses that are allowed to successfully communicate with the switch port are secure MAC addresses. The default number of secure MAC addresses is 1, but a maximum of 132 secure MACs can be configured.

When a non-secure MAC address attempts to communicate with the switch port, one of three actions will occur, depending on the port security mode. In Protect mode, frames with non-secure MAC addresses are dropped. There is no notification that a violation has occurred. The port will continue to switch frames for the secure MAC address.

In Restrict mode, the same action is taken, but a syslog message is logged via SNMP, which is a messaging protocol used by Cisco routers.

In Shutdown mode, the interface goes into error-disabled state, the port LED will go out, and a syslog message is logged. The port has to be manually reopened. Shutdown mode is the default port-security mode.

Port-based authentication is just one of the many switching skills you'll have to demonstrate to earn your CCNA certification. Make sure you know the basics shown here, including the action of each particular mode, and you're on your way to CCNA exam success!